VIII kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
(nr 68)
z dnia 28 września 2017 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 68)

28 września 2017 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Pawła Pudłowskiego (N)**, przewodniczącego Komisji, rozpatrzyła:

– informację Ministra Cyfryzacji o postępach prac nad rządowym projektem ustawy o krajowym systemie cyberbezpieczeństwa.

W posiedzeniu udział wzięli: **Krzysztof Silicki** podsekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Monika Bożyk** radca ministra w Departamencie Spraw Obywatelskich Ministerstwa Spraw Wewnętrznych i Administracji, **Adam Piotrowski** dyrektor Departamentu Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji wraz ze współpracownikami, **Arkadiusz Gawryś** główny specjalista w Departamencie Bezpieczeństwa i Ochrony Informacji Ministerstwa Finansów, **Andrzej Smoliński** zastępca dyrektora Biura Dyrektora Generalnego Ministerstwa Środowiska, **Anna Skibińska** zastępca dyrektora Biura Dyrektora Generalnego Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej, **Artur Brudziński** naczelnik w Biurze Dyrektora Generalnego Ministerstwa Kultury i Dziedzictwa Narodowego, **Bogdan Czekalski** główny specjalista w Departamencie Informatyki Ministerstwa Rozwoju, **Ewa Janczar** zastępca Dyrektora Departamentu Cyfryzacji, Geodezji i Kartografii Urzędu Marszałkowskiego, **Andrzej Kaczmarek** dyrektor Departamentu Informatyki Biura GIODO, prof. **Janusz Kawecki** członek Krajowej Rady Radiofonii i Telewizji, **Jacek Orzeł** dyrektor Departamentu Bezpieczeństwa i Zarządzania Kryzysowego Ministerstwa Rozwoju wraz ze współpracownikami, **Tomasz Jaskółowski** specjalista w Departamencie Żeglugi Śródlądowej Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej, **Joanna Maj-Marjańska** naczelnik Wydziału Prawnego w Departamencie Prawa i Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego, **Maciej Pyznar** szef Wydziału Ochrony Infrastruktury Krytycznej Rządowego Centrum Bezpieczeństwa, **Robert Tyszkiewicz** samodzielne stanowisko ds. obsługi legislacyjnej w Rządowym Centrum Bezpieczeństwa, **Piotr Balcerzak** pełnomocnik zarządu Związku Banków Polskich ds. Bankowego Centrum Cyberbezpieczeństwa, **Maciej Bułkowski** dyrektor Departamentu Społeczeństwa Informacyjnego Urzędu Marszałkowskiego Województwa Warmińsko- Mazurskiego w Olsztynie, **Paweł Dziuba** szef Inspektoratu Systemów Informacyjnych, **Dominik Dobek** przedstawiciel ZIPSEE „Cyfrowa Polska", **Joanna Karczewska** członek zarządu Stowarzyszenia ISACA Warszawa, **Piotr Marczuk** prezes Związku Pracodawców Technologii Cyfrowych Lewiatan, **Daniel Ślęzak** przedstawiciel Polskiej Izby Informatyki i Telekomunikacji, **Dominik Rozdziałowski** dyrektor Biura do Walki z Cyberprzestępczością Komendy Głównej Policji, **Albert Woźniak** ekspert w Departamencie Strategii Krajowej Rady Radiofonii i Telewizji, **Janusz Żmudziński** wiceprezes Polskiego Towarzystwa Informatycznego.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Anna Ornat** i **Julia Popławska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Paweł Pudłowski (N):

Dzień dobry, otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. Witam państwa posłów i zaproszonych gości. Stwierdzam kworum. Porządek dzisiejszego posiedzenia to rozpatrzenie informacji ministra cyfryzacji o postępach prac nad rządowym projektem ustawy o krajowym systemie cyberbezpieczeństwa. Powyższy porządek i materiały członkowie Komisji otrzymali. Czy są uwagi do porządku dziennego? Nie słyszę. Stwierdzam, że Komisja przyjęła porządek dzienny bez zmian.

Przystępujęmy do realizacji porządku dziennego. Uprzejmię proszę pana Krzysztofa Silickiego podsekreterza stanu w Ministerstwie Cyfryzacji o przedstawienie informacji.

Podsekretarz stanu w Ministerstwie Cyfryzacji Krzysztof Silicki:

Dzień dobry państwu. Dziękuję. Szanowny, panie przewodniczący i Wysoka Komisjo, jest mi niezwykle miło mieć okazję wystąpić tutaj przed państwem z tematem dotyczącym cyberbezpieczeństwa. Jestem debiutantem w tej roli, dlatego proszę mi wybaczyć, jeśli zdarzą się z mojej strony pomyłki. Są to też zresztą moje pierwsze dni w Ministerstwie Cyfryzacji, bo powołanie dostałem 5 września, tak więc mam krótkie doświadczenie w administracji. Natomiast od wielu, wielu lat zajmuję się tematyką cyberbezpieczeństwa.

Jeśli pan przewodniczący pozwoli, chciałbym powiedzieć kilka słów odnośnie do tego, co jest celem tego spotkania, czyli ustanowienie porządku legislacyjnego w nowej dziedzinie, jaką jest cyberbezpieczeństwo. Następnie, jeśli pan pozwoli, oddałbym głos panu dyrektorowi Januszewiczowi, który przedstawi krótką prezentację na ten temat.

Moim zdaniem istotne jest, aby niejako wyartykułować, że jesteśmy obecnie w takiej sytuacji, w której temat bezpieczeństwa teleinformatycznego, czy tak jak mówi się teraz, cyberbezpieczeństwa, zyskał i nadal zyskuje coraz większe zrozumienie i wagę we wszystkich krajach, również w naszym. Polska, jako członek Unii Europejskiej, jest zobowiązana do wprowadzania dyrektyw i regulacji. Jednym z celów ustawy o systemie cyberbezpieczeństwa, o którym będzie mowa, jest implementacja tzw. dyrektywy NIS – dyrektywy Unii Europejskiej o środkach służących wysokiemu wspólnemu bezpieczeństwu sieci i informacji na terenie Unii Europejskiej.

Nie jest to jedyny cel tej ustawy. Przynajmniej niektórzy z państwa pamiętają wnioski raportu Najwyższej Izby Kontroli, w których podkreślano, że potrzebny jest w naszym kraju system, który będzie koordynował pewne działania. Cyberbezpieczeństwo jest takim plastycznym przykładem oddziaływania horyzontalnego pomiędzy sektorami, jak i pomiędzy działami gospodarki. Jest to więc kwestia dodefiniowania kształtu całego cyberbezpieczeństwa. Mówimy głównie o sferze cywilnej, ale w taki sposób, by była synchronizacja z zadaniami związanymi z zarządzaniem kryzysowym, walką z cyberprzestępczością; jak również z zadaniami związanymi z tak zwaną cyberobroną. Różne resorty są zainteresowane wprowadzaniem określonych środków formalnych, organizacyjnych, ale też technologicznych, żeby podnosić poziom cyberbezpieczeństwa i zdolności do przeciwdziałania.

Projekt ustawy, który będziemy dziś charakteryzować, nie wziął się znikąd. Wcześniej nastąpiły działania związane z opracowaniem strategii cyberbezpieczeństwa, która przybrała postać krajowych ram polityki cyberbezpieczeństwa, przyjętych pod koniec kwietnia tego roku uchwałą Rady Ministrów. Z krajowych ram wynika, że musimy postawić sobie zadanie dostosowania systemu prawnego do wyzwań, jakie stoją przed naszym krajem w tej dziedzinie. Wynika z nich również tzw. plan działań. W ciągu 6 miesięcy, czyli do listopada tego roku, należy go opracować. Jest też sama propozycja, projekt ustawy, który głównie implementuje dyrektywę NIS, ale zawiera też szersze konteksty, o czym będzie mowa w prezentacji.

Dużo czasu zabrało znalezienie formuły współuczestniczenia poszczególnych interesariuszy, wszystkich ważnych resortów, żeby uwzględnić horyzontalny aspekt cyberbezpieczeństwa. Została wypracowana formuła zespołu międzyresortowego, który pracuje od wielu miesięcy – najpierw nad strategią, potem planem działań. W trakcie prac nad projektem ustawy latem tego roku odbyły się prekonsultacje. W ramach zespołu powstała grupa zadaniowa, która w tym momencie dosłownie kończy pracę nad modelem operacyjnej współpracy zespołów typu CERT poziomu krajowego. Są to trzy CERT-y plus Rządowe Centrum Bezpieczeństwa, Ministerstwo Spraw Wewnętrznych i Administracji. Moim zdaniem jest to sukces samego modelu, który wykorzystuje wiedzę, kompetencje, ale też daje możliwość wyartykułowania różnych potrzeb z różnych stron, różnych resortów. Zespół ten rzeczywiście potrafi wypracować dokumenty, na które jest zgoda ze strony ważnych, kluczowych graczy.

Oczywiście jest też tak, że istnieje konieczność zgodności z przepisami Unii Europejskiej. Sama dyrektywa została przez Parlament Europejski przyjęta w zeszłym roku.

Na uzyskanie zgodności legislacyjnej, czyli na transpozycję tej dyretywy, jest 21 miesięcy. To nie jest dużo w takim obszarze. Zresztą cały czas w ciałach Unii Europejskiej trwają prace nad dokumentami, które mają za zadanie wspomóc kraje członkowskie w implementacji. Dosłownie wczoraj czy przedwczoraj Komisja Europejska opublikowała rozporządzenie czy dokument, który póki co jest projektem, ale będzie obowiązujący, mówiący o kryteriach postępowania w stosunku do tzw. usługodawców czy dostawców usług cyfrowych. W ramach grupy współpracy europejskiej – jednego z pierwszych elementów wdrażania dyrektywy, która została uruchomiona po zaledwie 6 miesiącach od przyjęcia samej dyrektywy – działają trzy grupy robocze, ostatnio powstała czwarta. Pracują one nad stworzeniem rekomendacji dotyczącej tego, jak wdrażać dyrektywę. Z jednej strony, praca trwa bez czekania na rekomendację. Powiemy o tym, jak widzimy harmonogram. Z drugiej strony, cały czas jest to materia zmieniająca się dynamicznie. Nawet na poziomie Unii Europejskiej większość krajów jest w podobnej do naszej sytuacji, czyli konstruowane są projekty ustaw, które trafią do konstultacji, a następnie pod obrady parlamentu.

Na tym może zakończyłbym wprowadzenie i chciałbym teraz prosić pana dyrektora Januszewicza o zaprezentowanie tego, co przygotowaliśmy na slajdach.

Dyrektor Departamentu Cyberbezpieczeństwa MC Piotr Januszewicz:

Panie przewodniczący, szanowni państwo, tak jak mówił pan minister w swoim wystąpieniu, chciałbym poruszyć dwa aspekty: strategię cyberbezpieczeństwa, która z przyczyn formalnych przyjęła nazwę Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, i ustawę o krajowym systemie cyberbezpieczeństwa.

Jeśli chodzi o krajowe ramy polityki cyberbezpieczeństwa, chciałbym się skoncentrować głównie na tym, co zostało ustalone, jak zostało to zapisane. Wydaje się jednak, że równie ważny jest kontekst, o którym mówił pan minister: krajowe ramy polityki cyberbezpieczeństwa powstawały jako wynik pracy wielu ludzi z różnych resortów i to jest nasz dorobek wspólny, że ten dokument powstał. Ministerstwo Cyfryzacji było organizatorem zespołu, który pracował nad krajowymi ramami. Początek prac sięga wiosny 2016 r. Ministerstwo Cyfryzacji przygotowało materiały wyjściowe, tzw. draft stategii cyberbezpieczeństwa. We wrześniu dokument został przesłany do konsultacji. W grudniu został formalnie powołany zespół międzyresortowy, który miał za zadanie opracowanie tejże stategii. Jako materiał wyjściowy służył dokument, który przygotowaliśmy, natomiast w wersji końcowej został on gruntownie przemodelowany i przerobiony. Tak jak mówił pan minister, 9 maja tego roku pani premier podpisała uchwałę, dokument został przyjęty. Od tego czasu mamy 6 miesięcy na przygotowanie planu działania, dlatego że sama strategia, tak wolałbym to nazywać, bo jest to dokument w randze strategicznej, opisuje pewne kierunki działania, obszary, które chcemy zrobić. Natomiast plan realizacji będzie dokumentem, w którym będziemy mieli zapisane konkrety.

Jeśli chodzi o cel główny, który został sformułowany, jest to zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego i sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych. Istotna rzeczą w tym jest to, że myślimy tak naprawdę w kategoriach nie tylko sfery publicznej, mówimy o administracji, czy firmach prywatnych, ale myślimy też o obywatelach. Bowiem tylko współpraca wszystkich tych podmiotów i obywateli może doprowadzić do podniesienia poziomu bezpieczeństwa. Cel główny jest dość ogólny, dlatego został podzielony na cztery cele szczegółowe. Pierwszym z nich jest osiągnięcie zdolności do skoordynowanych w skali kraju działań. Wynikał on prawie bezpośrednio z zaleceń Najwyższej Izby Kontroli, która w swojej diagnozie stwierdziła, że na poziomie państwa trudno nam jest koordynować działania w zakresie utrzymania cyberbezpieczeństwa. Drugi cel to wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom. Chodzi o zbudowanie szeroko rozumianych kompetencji oraz tak naprawdę systemu, który pozwoli nam na przeciwdziałanie; nie tylko na wykrywanie czy skoordynowane działania, ale też przeciwdziałanie materializacji zagrożenia. Celem trzecim jest zwiększenie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni. Główne obszary w tym przypadku są zarówno technologiczne, jak i osobowe. Chodzi

o to, żeby wszyscy ci, którzy korzystają z systemów teleinformatycznych czy cyberprzestrzeni mogli bezpiecznie w niej funkcjonować, rozumieli zjawiska, a jednocześnie mieli do dyspozycji urządzenia, które są odpowiednio zabezpieczone i bezpieczne. Cel czwarty, który nam przyświecał, to zbudowanie silnej pozycji międzynarodowej Polski w zakresie cyberbezpieczeństwa. Mówimy tu o współpracy poszczególnych resortów na arenie międzynarodowej, koordynacji współpracy, abyśmy mówili jednym głosem, żebyśmy w tworzonych grupach roboczych bądź tych, które będą tworzone, aktywnie uczestniczyli, wnosili swoje zdanie i pomysły na realizację zadań w zakresie cyberbezpieczeństwa.

Tak jak powiedziałem, do krajowych ram przygotowywany jest plan. Jest on na ukończeniu. Zbudowany jest w ten sposób, że cel główny rozbity jest na cele szczegółowe. Do każdego celu szczegółówego mamy przypisane kierunki interwencji, a każdy z nich jest realizowany poprzez odpowiednie zadania. Zadania te mają charakter ciągły, są realizowane przez instytucje, wynikają z obowiązkow statutowych tych instytucji. Są też zadania o charakterze projektowym i mają na celu osiągnięcie konkretnych efektów, które są zapisane w strategii cyberbezpieczeństwa. Każde zadanie projektowe opisane jest fiszką projektową, w której określony jest cel zadania, co ma ono zrealizować, ile ma kosztować, jaki jest harmonogram realizacji.

Mamy nadzieję, że do 9 listopada wyrobimy się z tym wszystkim. Tak jak powiedziałem, jesteśmy już na ukończeniu tego dokumentu.Chcemy go niebawem wysłać do ostatecznych konsultacji międzyresortowych – aby wszystkie resorty potwierdziły to, co zgłaszały w planie wcześniej – i przedstawić go do zatwierdzenia.

Jeśli chodzi o kolejny obszar, tj. ustawę o krajowym systemie cyberbezpieczeństwa oraz implementację dyrektywy NIS, to najważniejsze jest to, jakie mamy wynikające z dyrektywy obowiązki. Przedstawię wybrane. Po pierwsze musimy doprowadzić do identyfikacji operatorów usług kluczowych oraz wymagań bezpieczeństwa teleinformatycznego dla tych operatorów. Kolejną sprawą jest wyznaczenie organów właściwych dla operatorów kluczowych. Przyjęliśmy założenie, o czym będę mówił później, że tworzymy system zdywersyfikowany, niezcentralizowany, w zakresie identyfikacji tych podmiotów. Wydaje nam się, że takie rozwiązanie jest najlepsze; żeby było ileś podmiotów właściwych, które będą to realizowały, a nie jeden. Kolejne zadanie, które przed nami stoi, to wyznaczenie pojedynczego punktu kontaktowego. Będzie on realizował współpracę międzynarodową, koordynował ją na poziomie krajowym, ale nie jest to element sticte techniczny, a bardziej strategiczno-polityczno-doradczy. Kolejną rzeczą jest wyznaczenie CERT-ów dla operatorów usług kluczowych i dostawców usług cyfrowych. Każdy z dostawców i operatorów musi mieć swoje systemy zabezpieczone poprzez tego typu usługi. Natępna sprawa: zbudowanie sieci wymiany i raportowania na poziomie Unii Europejskiej na temat poważnych incydentów u operatorów usług kluczowych oraz istotnych elementów u dostawców usług cyfrowych. Kolejnym zadaniem, jakie przed nami stoi jest przyjęcie w unijnej procedurze wymagań dla dostawców usług cyfrowych, dlatego że dostawcy usług cyfrowych będą regulowani innymi aktami prawnymi. Następną rzeczą, która jest na nas wymuszana, jest przyjęcie unijnej strategii bezpieczeństwa sieci i informacji. Myślimy, że uda się udowodnić, że wydana strategia będzie spełniała te wymagania. Jeśli byłyby w tym zakresie problemy, to zgodnie z zapisami strategii, co dwa lata jest przegląd, więc w przyszłym roku może zacząć inicjować przegląd strategii. Mam nadzieję, że to wypełnimy.

Jeśli chodzi o cel projektu, jest to wypracowanie uregulowań prawnych umożliwiających implementację dyrektywy NIS, ale tak naprawdę musimy podejść troszeczkę szerzej niż sama dyrektywa, ponieważ reguluje ona tylko pewne obszary. A my mamy ambitne plany, żeby utworzyć efektywny system bezpieczeństwa teleinformatycznego dla państwa. To jest cel, który nam przyświeca. Żeby cel ten zrealizować na poziomie krajowym, realizacją zadań jest niezakłócone świadczenie usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiedniego poziomu bezpieczeństwa dla owych usług.

Jeśli chodzi o główne podmioty, które do tej pory zidentyfikowaliśmy, są to przede wszystkim organy właściwe do spraw cyberbezpieczeństwa, czyli to, z czego będzie się składała ustawa, CSIRT-y poziomu krajowego, operatorzy usług kluczowych, dostawcy usług cyfrowych, pojedynczy punkt kontaktowy, inne zespoły reagowania na incydenty

typu CSIRT, mogą to być CSRIT-y wewnętrzne organizacji lub zewnętrzne, komercyjne, które bedą świadczyły odpowiednie usługi. Dla nas najważniejsze jest to, że każdy taki podmiot powinien mieć zabezpieczone funkcjonowanie swoich systemów przez zespoły typu CERT.

Kolejny obszar to Rządowe Centrum Bezpieczeństwa w zakresie zarządzania kryzysowego. Powinno ono odgrywać istotną rolę w zakresie usuwania skutków materializacji zagrożeń w cyberprzestrzeni, które będą miały wpływ na funkcjonowanie podmiotów, obywateli itd. Należy też podkreślić, że ustawa sama w sobie nie tworzy oddzielnego bytu. Państwo funkcjonuje w pewnym systemie bezpieczeństwa i obszary bezpieczeństwa tradycyjnego są dość dobrze uregulowane. Nasza ustawa natomiast musi się wkomponować w cały system bezpieczeństwa państwa i uzupełnić go o obszar związany z wykorzystywaniem nowych technologii do funkcjonowania w życiu codziennym.

Jeśli chodzi o to, co już powiedziałem, tj. o dyrektywie NIS, ale nie tylko, naszym projektem chcemy objąć podmioty, które nie są objęte dyrektywą NIS. Chodzi tutaj o programy rządowe z 7 września 1991 r. o systemie oświaty w zakresie podnoszenia kompetencji dzieci i młodzieży w obszarze bezpiecznego korzystania z technologi ICT. Kolejny obszar, który chcemy objąć, to włączenie administracji publicznej do systemu cyberbezpieczeństwa. Będzie taka sytuacja, w której część administracji publicznej, czy też część jej podmiotów stanie się jednocześnie operatorami usług kluczowych i to jak gdyby automatycznie zostanie objęte. Natomiast część podmiotów nie wchodziłaby w zakres tej ustawy. Uważamy, że administracja publiczna powinna również dołożyć należytej staranności do tego, aby systemy, które wykorzystuje do pracy, były należycie zabezpieczone. Istotna rola jest po stronie aglomeracji miejskich. Budujemy systemy smart city i tak naprawdę funkcjonowanie owych aglomeracji jest silne związane z funkcjonowaniem nowoczesnych technologii. Atak na nie może doprowadzić do paraliżu całych miast, w związku z powyższym obszar administracji, nazwijmy to, samorządowej też powinien być tym objęty.

Jeśli chodzi o architekturę takiego systemu, postaraliśmy się skoncentrować na jednym rysunku. Jest być może bardzo duża liczba elementów, które na nim jest i to może zamazywać obraz. Główni aktorzy, których tu widać, to są organy właściwe. W ramach organów właściwych mamy ministrów i ministerstwa, którzy w swoich kompetencjach mają poszczególne sektory wynikające z dyrektywy NIS. To jest ta część po prawej stronie, gdzie mamy banki, infrastrukturę rynków finansowych, energię, infrastrukturę cyfrową i komunikacyjną, transport, instalacje wodno-kanalizacyjne, dostawców usług cyfrowych i obszar zdrowia. Na dzień dzisiejszy mamy taki zamysł, żeby organami właściwymi do tego byli ministrowie właściwi w tym zakresie. Natomiast chcemy zapisać też takie kompetencje, żeby ministrowie mogli powierzyć to innym organom, które im podlegają i są przez nich nadzorowane, np. regulatorzy, którzy mogliby przejąć tę rolę. Chcielibyśmy jednak, żeby odpowiedzialność spoczywała na ministrach. Dajemy im jednak swobodę dysponowania, żeby tam gdzie mają najlepsze kompetencje mogli przekazać zadania związane z wykonywaniem tego obszaru.

Po lewej stronie mamy administrację i jej działy. Mamy np. Ministerstwo Obrony Narodowej, które jest działem obrony narodowej; mamy Ministerstwo Sprawiedliwości, Spraw Wewnętrznych i Administracji. To są te obszary administracyjne, co do których uważamy, że też powinny zostać objęte tym systemem. Do tego, tak jak już mówiliśmy przy okazji strategii, musimy stworzyć efektywny system współpracy i skoordynowanych działań. W tym celu niezbędne jest naszym zdaniem zbudowanie sieci CSIRT poziomu krajowego. W ramach CSRIT poziomu krajowego widzimy tutaj główną rolę Ministerstwa Obrony Narodowej. Nazywamy to… To byłby CERT Ministerstwa Obrony Narodowej, CERT Agencji Bezpieczeństwa Wewnętrznego, czyli cert.gov.pl, oraz CERT, który jest zlokalizowany w Naukowej i Akademickiej Sieci Komputerowej (NASK).

Tworzyłyby one podstawę do koordynowania wszystkich działań w zakresie bezpieczeństwa i incydentów, które powstaną. Oprócz tego niezbędne jest zaangażowanie organów ścigania. Mówiliśmy o skutecznym przeciwdziałaniu, w związku z tym organy ścigania w postaci policji, prokuratury muszą mieć swoją istotną rolę. Chodzi nam o zbudowanie takiego systemu, w którym czas pomiędzy lokalizacją zagrożenia a czasem prze-

ciwdziałania, będzie zminimalizowany do poziomu dającego się uregulować w prawie; żeby te organy działały zgodnie z prawem. Tak bowiem musimy tworzyć ten system.

Jeżeli chodzi o następne elementy, to mamy Ministerstwo Cyfryzacji, w którym chcemy zlokalizować pojedynczy punkt kontaktowy; będzie on realizował współpracę międzynardową w ramach grupy współpracy. Dalej jest Rządowe Centrum Bezpieczeństwa, które jest właściwie w zakresie zarządzania kryzysowego i stanowi swoisty sztab w zakresie rządowego zespołu zarządzania kryzysowego. Są też oczywiście prezes Rady Ministrów i prezydent. A to dlatego, że musimy stworzyć taki system, który przewiduje funkcjonowanie w różnych stanach bezpieczeństwa państwa. Mam tu na myśli czas pokoju, kiedy główny obszar skoncentrowany jest na przestępczości pospolitej, mamy elementy działań hybrydowych, wojny informacyjnej, ale z punktu widzenia prawnego mimo wszystko jest to jeszcze stan pokoju.

Musimy być również przygotowani na wypadek ataków terrorystycznych. Właśnie po to potrzebne jest wkomponowanie naszego systemu w cały system prawny; żeby można było aktywować inne środki reagowania. Na samym końcu jest stan wojenny i stan wojny, najgorszy, w jakim państwo może się znaleźć. Widzimy tu zgodnie z prawem rolę pana prezydenta. Jeśli chodzi o poziom odcięcia technicznego i strategiczno-politycznego, widzimy to między CSRIT-ami poziomu krajowego a Rządowym Centrum Bezpieczeństwa. A to dlatego, że poziom techniczny może wyłącznie neutralizować czy minimalizować to, co dzieje się w zakresie cyberprzestrzeni. Natomiast najczęściej dochodzi do takiej sytuacji, w której materializacja zagrożeń w cyberprzestrzeni ma bezpośredni, fizyczny wpływ na funkcjonowanie przedsiębiorstw i obywateli. Dlatego też zajmujemy się cyberprzestrzenią: to jest coś, co dotyka nas bezpośrednio, ponosimy określone straty, przedsiębiorstwa ponoszą określone straty, państwo ponosi określone straty, kiedy znajduje się w stanie bądź znajduje się w stanie określonego zagrożenia. Ścieżka reagowania na to musi być tak zorganizowana, żeby we wszystkich stanach bezpieczeństwa państwa działało to automatycznie. W związku z powyższym, tak jak mówię, musimy się wkomponować w cały ten system.

Jeśli chodzi o obsługę incydentów, to wyobrażamy sobie w ten sposób, że w momencie, w którym zmaterializują się zagrożenia w przedsiębiorstwach czy metropoliach, zadziałają regionalne centra cyberbezpieczeństwa, które będą obejmowały ileś podmiotów administracji samorządowej. Wszystko to będzie obsługiwane przez CERT-y lub ISAC-i wyspecjalizowane w zabezpieczaniu czy rozwiązaniu problemów, związanych z cyberatakami. Myślimy również o tym, żeby owe podmioty były zabezpieczone przez centra operacyjne cyberbezpieczeństwa – security operations centre. Jeśli one wykryją jakikolwiek incydent, zdefiniują, że jest poważny, to raportują go na sieć poziomu CERT -ów krajowych i chcielibyśmy, żeby wszystkie CERT-y dostawały informację, a na podstawie podziału kompetencji było wiadomo, który CERT czymś się dokładnie zajmuje i jaki rodzaj incydentów obsługuje. Natomiast w przypadku stwierdzenia, że atak ten może mieć istotny wpływ na funkcjonowanie podmiotów gospodarczych, państwa czy obywateli, informacja cały czas musi być dostarczana do Rządowego Centrum Bezpieczeństwa. A ono jako ciało, które będzie przetwarzało dane i sprawdzało, jaki to ma wpływ na fizyczny byt podmiotów, będzie raportowało dalej czy zalecało wprowadzenie określonych środków. Wejdziemy wtedy w system zarządzania kryzysowego czy system innych stanów bezpieczeństwa państwa.

Jeśli chodzi o pojedynczy punkt kontaktowy, to tak jak już powiedziałem na wstępie, chcemy go zlokalizować w Ministerstwie Cyfryzacji. Zasilenie informacyjne będzie miał z CSIRT- u poziomu krajowego i główną jego rolą będzie broker informacyjny dla wszystkich interesariuszy w krajowym systemie informacyjnym. Chcielibyśmy doprowadzić też do takiej sytuacji, w której przedsiębiorstwa czy podmioty będą miały jedno miejsce, do którego będą zgłaszały tak naprawdę informacje o incydentach. A ten incydent, jeśli będzie np. dotyczył ochrony danych osobowych, zostanie przekazany do wszystkich instytucji, które powinny uzyskać taką informację. Jeśli będzie miał charakter działań terrorystycznych lub będą objawy działań terrorystycznych, to chodzi o to, żeby odpowiednie organy to dostały. Chcemy też doprowadzić do tego, żeby nie było sytuacji,

w których przedsiębiorca jest zobowiązany do raportowania w ileś miejsc na innych formularzach, na innych arkuszach i zupełnie innych obszarach.

Kolejną rzeczą, którą chcemy by realizował pojedynczy punkt kontaktowy, jest kontrola spełnienia przez CSIRT-y wymagań organizacyjnych i technicznych. Jest to istotna funkcja, ponieważ będą one zabezpieczały podmioty, które są istotne z punktu widzenia interesów społeczno-gospodarczych kraju. W związku z powyższym uważamy, że powinny podlegać kontroli organizacyjnej, technicznej oraz kwalifikacji w zakresie bezpieczeństwa czy rozwiązywania problemów związanych z bezpieczeństwem.

Następnym elementem jest gromadzenie i przetwarzanie informacji z organów właściwych. Chcemy stworzyć pojedynczy punkt. Organy właściwe bedą przekazywały wszystkie informacje na temat operatorów usług kluczowych i dostawców usług cyfrowych do pojedynczego punktu kontaktowego. Będzie on miał wszystkie informacje na temat operatorów i dostawców.

Następnie jest funkcja łącznika w celu zapewnienia współpracy transgranicznej w zakresie wymiany informacji pomiędzy państwami Unii Europejskiej; kolejną jest tworzenie ram prawnych funkcjonowania obszarów cyberbezpieczeństwa państwa. Zdajemy sobie sprawę, że życie nowych technologii dość mocno się zmienia i zagrożenia bardzo szybko ewoluują, w związku z czym ustawa musi ciągle żyć, a nie być skończoną i działać na zasadzie, że więcej się do niej nie wróci. Musimy monitorować skuteczność zaimplementowanych środków i podejmować stosowne działania, żeby doskonalić system.

Następnie jest realizacja zadań edukacyjno-informacyjnych, czyli tak naprawdę inspirowanie i inicjowanie określonych przedsięwzięć związanych z zadaniami informacyjno -edukacyjnymi. Jeśli chodzi o zadania organów właściwych, jest to prowadzenie analiz podmiotów w danym sektorze pod kątem uznania określonych podmiotów za operatorów usług kluczowych czy dostawców usług cyfrowych. Jeżeli na podstawie kryteriów i progów odcięcia stwierdzą, że dany podmiot spełnia te kryteria i punkty odcięcia, następuje wydawanie decyzji o uznaniu podmiotu za operatora usługi kluczowej lub dostawcę usługi cyfrowej.

W momencie, kiedy decyzje te zostaną wydane, ma miejsce przekazanie informacji do pojedynczego punktu kontaktowego, żeby ująć podmiot w wykazie. Za pośrednictwem pojedynczego punktu kontaktowego mogą również prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej. Chodzi o to, żeby na poziomie Unii Europejskiej doprowadzić, tak jak mówi dyrektywa, do wspólnego poziomu bezpieczeństwa, a jak zapewnić Unii bezpieczeństwo najlepiej wiedzą sektory. W związku z powyższym przez pojedynczy punkt kontaktowy powinny się kontaktować ze swoimi odpowiednikami w innych państwach, a także przetwarzać informacje dotyczące świadczonych usług kluczowych oraz operatorów usług kluczowych i uczestniczyć w ćwiczeniach w zakresie cyberbezpieczeństwa uruchamianych na poziomie Unii Europejskiej i w kraju.

Jeśli chodzi o harmonogram prac, to robocze uzgodnienia z przedstawicielami resortów miały miejsce w lipcu i we wrześniu. W tej chwili jesteśmy po procesie obróbki wszystkich zgłoszonych uwag. Było około osiemdziesięciu stron z dwustu kilkudziesięcioma uwagami.

Jeśli chodzi o uzgodnienia, konsultacje publiczne i opiniowanie, zamierzamy przekazać projekt w październiku/listopadzie 2017 r. Analizę uwag, które do nas wpłyną, chcielibyśmy zakończyć w listopadzie/grudniu 2017 r. Komitetowi Rady Ministrów do Spraw Cyfryzacji przekazać w grudniu 2017 r., Komitetowi do Spraw Europejskich Rady Ministrów też w grudniu 2017 r., stałemu Komitetowi Rady Ministrów w styczniu 2018 r., Komisji Prawniczej w styczniu 2018 r., Radzie Ministrów w lutym 2018 r. Do prac w parlamencie chcielibyśmy przekazać projekt na przełomie lutego i marca 2018 r. Jeśli wszystko dobrze by poszło, w kwietniu pan prezydent mógłby podpisać gotową ustawę. Dziękuję za uwagę. To tyle, ile chciałem państwu przekazać.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję, panie ministrze. Bardzo dziękuję, panie dyrektorze. Otwieram dyskusję. Pan przewodniczący Czarnecki, bardzo proszę.

Poseł Witold Czarnecki (PiS):

Dziękuję bardzo, panie przewodniczący. Panie ministrze, jest oczywiste, że jako państwo unijne musimy dostosować się do dyrektywy NIS. Różne państwa w różny sposób to czynią. Postęp prac w całej Europie wygląda różnie. Wybraliśmy nieco inny wariant niż Francja czy Niemcy. W przypadku Niemiec jednostką wiodącą i koordynatorem głównym jest Federalny Urząd do spraw Bezpieczeństwa Techniki Cyfrowej, podlegający bezpośrednio Federalnemu Ministrowi Spraw Wewnętrznych. Z kolei we Francji jest jedna agencja, ANSII, która mocno identyfikuje cele szczegółowe. Chciałbym zwrócić uwagę na jedną rzecz, która jest moim zdaniem mocno niepokojąca. Francuzi w swojej strategii już w pierwszym punkcie podają, że chcą zapewnić Francji pozycję światowej potęgi w cyberbezpieczeństwie. Potęgi nie buduje się za darmo, potęga kosztuje. My w tej chwili jesteśmy na etapie budowy ram prawnych i to na pewno jest bardzo ważne, bo czymś musimy się zabezpieczyć. W naszej strategii w punkcie czwartym jest wymienione, że mamy być dosyć silnym państwem. Francja mówi o byciu potęgą w cyberobronie.

Polska jest państwem skrajnym, granicznym NATO i jesteśmy narażeni pewnie na więcej zagrożeń niż Francja. Jesteśmy też słabszym państwem, mamy zdecydowanie mniejszą potęgę. Nasz rząd powinien jednak znaleźć na to pieniądze, bo nie zbudujemy bezpieczeństwa państwa samą ustawą. Ustawa to tylko ramy prawne, a trzeba to wszystko wypełnić jeszcze materialną treścią.

Dobrze, że jest taka odpowiedź ministerstwa na krytyczny raport NIK z września 2015 r. Dobrze, że reagujemy. Mamy jeszcze trochę czasu na budowę ram prawnych, bo do maja trzeba skończyć pracę nad ustawą, a podmioty kluczowe trzeba określić do listopada 2017 r. Mamy więc czas, ale musimy zrobić wszystko, żeby wszystkim posłom uświadomić konieczność przeznaczenia na budowę dobrej, przyzwoitej pozycji wielkich środków. Prawdę powiedziawszy, nigdzie ich nie widać, w żadnym materiale. Korzystanie wyłącznie ze środków NCBR czy jakichś grantów na pewno nie zbuduje potęgi, ale nawet nie pozwoli na zbudowanie przyzwoitej i silnej pozycji. Uczulam więc pana, panie ministrze, i apeluję o to, by naciskać na rząd, uświadamiać, że to jest tak ważne. Bez pieniędzy tego nie zrobimy, a zagrożenia są wielostronne. Rozwój cyfryzacji i nowoczesnych technologii powoduje, że będą one tylko narastać, a nie się kurczyć. Musimy poszukiwać przyszłościowych, dobrych rozwiązań. Chciałbym tylko zaapelować o znalezienie źródła finansowania, bo nie widać tu żadnych finansów, nie pojawiają się one w tym projekcie. Mamy tylko ramy prawne. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Może dodam tylko, że chciałbym dowiedzieć się, ile w budżecie na 2018 r. przewidziano w Ministerstwie Cyfryzacji i w Ministerstwie Obrony Narodowej.

Zbierzemy pytania, a potem będą odpowiedzi. Pan poseł Marchewka, bardzo proszę.

Poseł Arkadiusz Marchewka (PO):

Dziękuję, panie przewodniczący. Szanowny panie ministrze, szanowni państwo, temat, o którym mówimy jest kluczowy. Już pierwsze informacje na temat dokumentu, który miał nazywać się strategią cyberbezpieczeństwa, zostały przedstawione pod koniec 2016 r. Prace przeciągnęły się o ponad rok. Miejmy nadzieję, że dokument uda się przyjąć bez kolejnej zwłoki.

Myślę, że kluczowe w tym zakresie jest wdrożenie planu działań na rzecz realizacji krajowych ram cyberbezpieczeństwa. Bez tego planu strategia pozostanie po prostu pustym dokumentem. Kluczowe jest to, w jaki sposób administracja rządowa, interesariusze całego otoczenia i systemu będą dążyć do tego, aby cel główny i cele szczegółowe w tym zakresie realizować. Dlatego chciałbym zadać kilka pytań i odnieść się do spraw, które mnie zasadniczo interesują.

Po wysłuchaniu tego, co pan dyrektor przedstawił na prezentacji, widać, że cyberbezpieczeństwo jest grą zespołową i uważam, że w systemie powinien funkcjonować jeden koordynator, który powinien odpowiadać za całość procesów. Oczywiście są różne modele zarządzania cyberbezpieczeństwem, ale też mieliśmy okazję uczestniczyć w jednym z forów cyberbezpieczeństwa, gdzie rzeczywiście takie rekomendacje zostały wskazane. Moje zasadnicze pytanie jest o to, kto będzie odgrywał kluczową rolę w tym procesie?

Chodzi o proces koordynatora. Osobiście uważam, że powinien nim być minister odpowiedzialny za sprawy informatyzacji, czyli Ministerstwo Cyfryzacji, natomiast ostatnio widzimy, że w tym zakresie dochodzi do pewnej, powiem to wprost, walki o wpływy pomiędzy Ministerstwem Obrony Narodowej a Ministerstwem Cyfryzaji. Ja uważam, że kluczową rolę powinien odgrywać minister cyfryzacji. To po pierwsze.

Druga kwestia dotyczy jednego z celów szczegółowych, który mówi o udoskonaleniu struktury krajowego systemu cyberbezpieczeństwa. W tym celu zawierają się takie szczegółowe kwestie jak określenie zakresu odpowiedzialności podmiotów koordynujących krajowy system cyberbezpieczeństwa, obowiązki i uprawnienia uczestników tego systemu czy sposób oddziaływania koordynatora na uczestników. Nawiązuję do tego, kto będzie odgrywał kluczową rolę koordynatora.

Wielokrotnie mówiliśmy o stworzeniu jednego punktu kontaktowego, który ma dotyczyć między innymi współpracy transgranicznej. Bardzo bym chciał, żeby panowie uszczegółowili tę kwestię, bo nie wiem, czy dobrze rozumiem. Dzisiaj ten system alertowania jest generalnie bardzo rozproszony, np. sektor instytucji publicznych zgłasza się do NC Cyber, a instytucje prywatne do Agencji Bezpieczeństwa Wewnętrznego, jeśli dobrze pamiętam. Widać, że w tej kwestii jest duże rozproszenie. Czy w takim razie jeden punkt kontaktowy dotyczy też kwestii alertowania i zgłaszania przez instytucje publiczne i sektor prywatny zagrożeń, które z tego wynikają?

Druga kwestia dotyczy roli koordynatora, o czym wspomniałem. Co jest dla mnie równie dyskusyjne, to podział kompetencji pomiędzy różne resorty. Kilka tygodni temu minister obrony narodowej powiedział, że tworzy biuro ds. organizacji polskich oddziałów cybernetycznych, na co planuje przeznaczyć w najbliższym okresie, nie sprecyzował w jakim, 2 mld złotych. To bardzo duża suma. Szczególnie w kontekście tego, że kiedy uchwalaliśmy budżet na 2018 r., pani minister Streżyńska mówiła, że na realizację działań związanych z wdrożeniem strategii na ten rok potrzebujemy 60 mln zł, ale nawet tych pieniędzy nie udało się zabezpieczyć w budżecie. Porównując 60 mln zł, których niby nie ma, i akcję ministra obrony narodowej, który znajduje 2 mld zł, jest to zastanawiające. Chciałbym więc zapytać o podział kompetencji, które ścierają się, tak mogę powiedzieć.

Trzecia kwestia, o którą chciałbym zapytać, dotyczy jednego z celów szczegółowych. Chodzi o wzmacnianie zdolności do przeciwdziałania zagrożeniom. Chciałbym zapytać, jak w kontekście realizacji tego celu zostanie zagwarantowane prawo do prywatności użytkowników sieci. Jest to niezwykle istotne. W całym procesie oczywiście unika się przeciwdziałania zagrożeniom, a później ich niwelowania. Nie możemy zapominać o tym, że bezpieczeństwo i prywatność użytkowników sieci powinny być w tym procesie kluczowe i zachowane.

Czwarta, ostatnia kwestia, dotyczy celu szczegółowego w zakresie edukowania i informowania. Uważam, że to bardzo istotne, żeby przeprowadzać kampanie edukacyjne, które będą uświadamiać Polakom, na jakie zagrożenia mogą napotkać korzystając z sieci. Z tych zagrożeń często nie zdają sobie sprawy. Wielu z nas nie zdaje sobie sprawy, jak bardzo jest narażonych na takie zagrożenia jak fishing itd. Dlatego chciałbym zapytać o jedną kwestię. Nie wiem, czy jest miejsce dla takiego działania w krajowych ramach, ale czy nie warto w jakiś sposób włączyć kwestii związanych z cyberbezpieczeństwem, ale w kontekście przeciwdziałania cyberprzemocy? W sposób szczególny dotyka ona nastolatków i dzieci. Dzisiaj młodzi ludzie, nastolatkowie są praktycznie non stop wpatrzeni w swoje smartfony i cały czas są dostępni w sieci, to jest ich alternatywna rzeczywistość. Wielokrotnie słyszeliśmy o różnych działaniach związanych z próbami samobójczymi i samobójstwami wynikającymi ze stalkingu, z tego, że młodzi ludzie byli wyśmiewani. Chodzi nawet o ostatni przypadek nastolatka, który popełnił samobójstwo, dlatego że był wyszydzany przez swoich rówieśników, między innymi w ten sposób.

Miasto Gdynia, jako jedne, nie wiem, czy jedyne, przyjęło uchwałą rady miasta, miejski plan przeciwdziałania cyberzagrożeniom, wynikających z kwestii, o których mówiłem. Są tam przeprowadzane akcje informacyjne, edukacyjne, uświadamiające. Zastanawiam się, czy na tę kwestię nie warto byłoby zwrócić uwagi. Uważam, że jest to coraz bardziej znaczący problem, który dotyczy coraz większej grupy młodych ludzi.

Myślę, że w kwestii cyberbezpieczeństwa nie należy patrzeć tylko na sprawę bezpośrednich zagrożeń, cyberataków, ale także na kwestie wynikające z cyberprzemocy. Warto w działaniach dotyczących edukowania i informowania mówić o tych kwestiach. Chciałbym więc zapytać pana ministra i pana dyrektora, czy działania również w tym zakresie są przewidziane? To są wszystkie kwestie, o które chciałem zapytać. Dziękuję.

Przewodniczący poseł Paweł Pudłowski (N):

To są bardzo dobre pytania. Na razie na tym zakończymy i będę prosił o odpowiedzi, a potem może uzbieramy jeszcze jakieś pytania. Bardzo proszę, panie ministrze.

Podsekretarz stanu w MC Krzysztof Silicki:

Dziękuję bardzo za te pytania, ponieważ one w istocie trafiają w sedno tego, z czym się wielokrotnie borykamy. To, co powiedział pan przewodniczący na temat modeli, jakie są przyjmowane w takich krajach jak Francja, Wielka Brytania czy Niemcy, to rzeczywiście widać, że tam idą za tym spore budżety. Jeśli zdamy sobie sprawę, że ANSII to jest 500 osób i ta liczba rośnie… to zdaje się jest 700... W Niemczech specyfiką jest federalność kraju.

Niemniej jednak zgadzam się w zupełności. Mogę się tylko obiema rękami podpisać pod tym, co powiedział pan przewodniczący. To rzeczywiście jest kwestia na poziomie strategicznym kraju, zdecydowania się nie tylko od strony opisowej, tworzenia dokumentów, które mówią o priorytetach i działaniach, które chcemy podjąć. Tak naprawdę namacalnym sprawdzeniem tego, jaką wagę chcemy przyłożyć, jest budżet, który jesteśmy skłonni alokować do tych działań. Na pewno jest jeszcze przed nami wiele pracy, żeby tworzyć taką świadomość, że nie jest to źle poniesiony wydatek, a inwestycja w przyszłość. Za parę lat na pewno będzie to element funkcjonowania biznesowego, funkcjonowania każdego podmiotu, który będzie chciał podejmować jakąkolwiek działalność. ICT i cyberbezpieczeństwo będą po prostu kluczowe. Wtedy wiele takich podmiotów zapyta, co zrobiło państwo? Jak przysłużyło się, żeby wspomóc wzrost w dziedzinie odporności na cyberzagrożenia?

Zapytał pan, ile tak naprawdę zostało przeznaczone w budżecie na 2018 r. Mogę się wypowiadać tylko za Ministerstwo Cyfryzacji, aczkolwiek padały liczby na temat tego, ile przeznacza Ministerstwo Obrony Narodowej na kwestie cyberobrony.

Przewodniczący poseł Paweł Pudłowski (N):

Zaraz dopytamy przedstawiciela MON, bo jest na sali.

Podsekretarz stanu w MC Krzysztof Silicki:

Rzeczywiście jest kwestia taka, że na posiedzeniach rządu ten element był już kilkukrotnie poruszany. Z tego, co wiem ostatnio po razu drugi niejako zostało powiedziane, że dedykowanego budżetu dla Ministerstwa Cyfryzacji na działania związane z wdrażaniem strategii raczej nie będzie. W porozumieniu z Ministerstwem Obrony Narodowej można liczyć na to, że, kolokwialnie mówiąc, zostanie wykrojony jakiś pewnie niewielki budżet, żeby można było to realizować.

Było tak, że pani minister Streżyńska występowała o uruchomienie rezerwy na przyszły rok. Była to kwota rzędu 60-70 mln zł. Zobaczymy, jak to się dalej potoczy. Nie mam informacji, że jest to proces zakończony. Tak jak pan przewodniczący powiedział, są jeszcze inne źródła finansowania – na pewno Narodowe Centrum Badań i Rozwoju. Uruchamiane tam programy dla cyberbezpieczeństwa są źródłem, o które chodzi. Powstał program CyberSecIdent, w ramach którego działania, o których mówiliśmy poprzednio, na pewno będą finansowane. O niektórych wiemy, że na pewno będą finansowane, np. powstanie narodowej platformy cyberbezpieczeństwa – kluczowego elementu do kolekcjonowania i wymiany informacji o zagrożeniach, analizy ryzyka itd. Oczywiście źrodło w postaci programów NCBR jest bardzo istotne.

Są też oczywiście programy unijne, które zawierają… cyberbezpieczeństwa i wręcz należy korzystać z tamtych pieniędzy. Jest to taki trochę patchwork finansowy do zrobienia. Istotne jest to, żeby wiedzieć, ile się ma. Wtedy można zacząć mówić, że dane zadania jesteśmy w stanie zrobić w 2018 r., ale muszą być kolejne lata. Strategia jest do 2020 r.

Przewodniczący poseł Paweł Pudłowski (N):

Panie ministrze, czy ja dobrze zrozumiałem, że nie ma alokacji bezpośrednio na cyberbezpieczeństwo w planowanym na 2018 r. budżecie w zakresie Ministerstwa Cyfryzacji?

Podsekretarz stanu w MC Krzysztof Silicki:

Pani minister Streżyńska powiedziała, że jest generalnie zadowolona z budżetu, jeśli chodzi o kwestie, które dotyczą i governmentu i projektów cyfryzacyjnych. Nie jest usatysfakcjonowana częścią dotyczącą cyberbezpieczeństwa.

Przewodniczący poseł Paweł Pudłowski (N):

Bo jej nie ma? Jest zero.

Podsekretarz stanu w MC Krzysztof Silicki:

Miejmy nadzieję, że się pojawią.

Przewodniczący poseł Paweł Pudłowski (N):

Mam wobec tego pytanie do pana ministra Grabskiego. Czy jest na sali? Mam potwierdzenie, że wszedł. Nie ma. A czy jest ktoś z Ministerstwa Obrony Narodowej?

Szef Inspektoratu Systemów Informacyjnych – Ministerstwo Obrony Narodowej Paweł Dziuba:

Tak, panie przewodniczący.

Przewodniczący poseł Paweł Pudłowski (N):

Mam prośbę: czy może się pan jakoś ustosunkować do tej kwoty, która padła? Chodzi o 2 mld zł, które w jakimś czasie będą dostępne dla Ministerstwa Obrony Narodowej na cyberzagrożenia i cyberbezpieczeństwo.

Szef ISI Paweł Dziuba:

Szanowny panie przewodniczący, szanowni państwo, nazywam się Paweł Dziuba. Jestem szefem Inspektoratu Systemów Informacyjnych.

Na początku chciałbym zaznaczyć coś, co pewnie wszystkim państwu jest znane: zakończenie szczytu NATO w Warszawie i podjęte decyzje w zakresie cyberbezpieczeństwa. Cyberprzestrzeń stała się kolejną domeną operacyjną automatycznie z punktu widzenia NATO i wszystkich państw, również Polski. Oznacza to, że jest zielone światło na poziomie NATO do tworzenia wojsk cybernetycznych. Tak jak zdają sobie państwo sprawę, wojska cybernetyczne, jak wszelkiego rodzaju udział w ramach NATO, to jest wkład poszczególnych członków. Innymi słowy: każde z państw, również Polska, zostaje zobowiązane w ten sposób do tworzenia odpowiednich sił zarówno w zakresie obrony, jak i aktywnej obrony. W tym celu odpowiednie środki i działania zostały rozpoczęte zarówno przez Polskę, jak i innych członków.

Jeśli chodzi o Ministerstwo Obrony Narodowej, oznacza to dla nas, co podkreślał pan minister, pracę nad stworzeniem pełnego spektrum możliwości w zakresie działań w cyberprzestrzeni w ramach obronności. Jeśli chodzi o budżet, to bardzo przepraszam, panie przewodniczący, ale nie mogę dokładnie odpowiedzieć na pana pytanie. Postaram się natomiast odpowiedzieć pisemnie. Niemniej tak, są przeznaczone środki finansowe, ponieważ, tak jak zostało podkreślone, powstaje biuro do tworzenia wojsk cybernetycznych. Innymi słowy: są na to potrzebne cele, aby nasze zdolności w zakresie bezpieczeństwa w cyberprzestrzeni były odpowiednio zabezpieczone. W tym celu zostały podjęte działania. One trwają. Szczyt NATO w pewnym sensie sformalizował to, co było, jest i musi być realizowane.

Chciałbym tylko podkreślić, że Ministerstwo Obrony Narodowej czynnie współpracuje z Ministerstwem Cyfryzacji. Myślę, że nie tylko nasze ministerstwo, ale i inne mają naprawdę dużo wspólnej pracy do wykonania i obszar ten wymaga raczej konsolidacji niż dzielenia. Ministerstwo Obrony Narodowej odpowiada za obronność, a cyberprzestrzeń jest jednym z elementów tejże obronności. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Dziękuję. Żebym dobrze zrozumiał – pan mówi, że jest budżet dedykowany na stworzenie kompetencji krajowych, a nie na składkę do NATO, które gdzieś tworzy siły, tak? One będą u nas, złożone z naszych żołnierzy, jak rozumiem.

Szef ISI Paweł Dziuba:

Tak, panie przewodniczący. Jak najbardziej. Jeżeli mamy siły i środki, którymi dysponujemy, to ewentualnie możemy istniejące, stworzone przez nas, siły i środki w pewien sposób delegować, jeżeli jest taka potrzeba i będzie taka prośba na rzecz członków wspólnoty. Niemniej tak, jak najbardziej mówimy tu o środkach na nasze narodowe potrzeby.

Przewodniczący poseł Paweł Pudłowski (N):

Znakomicie. Mam jeszcze pytanie precyzujące. Nie wiem, czy będzie pan skłonny odpowiedzieć. Czy jeśli postawiona została hipoteza co do organu koordynującego cyberbezpieczeństwo w Polsce i wskazania na Ministerstwo Cyfryzacji, to czy Ministerstwo Obrony Narodowej również widzi to w podobny sposób?

Szef ISI Paweł Dziuba:

Ministerstwo Obrony Narodowej w zakresie działań w cyberprzestrzeni wychodzi przede wszystkim z punktu widzenia zadań, jakie wynikają z obronności i z ustawy. To jest nasz punkt wyjścia. Wychodząc stąd, automatycznie rozszerzamy nasze działania i kompetencje we współpracy z innymi. Natomiast punktem wyjścia jest obronność. I to, co zostało już powiedziane, na czas „P", przy czym w cyberprzestrzeni trudno określić, co znaczy czas „P", ale na czas kryzysu i wojny istotne jest, abyśmy mieli odpowiednie kompetencje przez to, co jest do wykorzystania w ramach Ministerstwa Obrony Narodowej. Dlatego też budujemy kompetencje i patrzymy z punktu widzenia obronności państwa.

Przewodniczący poseł Paweł Pudłowski (N):

Rozumiem, bardzo dziękuję w tej sprawie, bo zaraz jeszcze wrócimy do odpowiedzi na pozostałe pytania. Pan Adam Cyrański, bardzo proszę.

Poseł Adam Cyrański (N):

Chciałem panu ministrowi zadać pytanie: czy to będzie polegało na tym, że owe 2 mld zł zaabsorbuje MON, a Ministerstwo Cyfryzacji będzie się prosić o 60 mln zł? Czy też nastąpi jakiś przepływ kapitału do budżetu Ministerstwa Cyfryzacji?

Szef ISI Paweł Dziuba:

Tak jak wspomniałem na początku, nie jestem na tę chwilę przygotowany, jeśli chodzi o mówienie o kwotach. Natomiast odpowiedź na to pytanie prześlę też na ręce pana przewodniczącego.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Bardzo przepraszam, panie ministrze. Wracamy wobec tego do odpowiedzi na pozostałe pytania.

Podsekretarz stanu w MC Krzysztof Silicki:

Jeszcze może odniosę się do tego, co zostało powiedziane na temat roli koordynacyjnej. Podkreślamy jednak, że zależy nam na federacyjnym modelu, w którym... Opowiadałem o tym, że jest taka grupa zadaniowa, która określa kompetencje i współpracę pomiędzy trzema CERT-ami poziomu krajowego. To naprawdę jest tak, że owa współpraca istnieje i to nie od wczoraj czy dziś.

Natomiast model jest taki, że każdy z CERT-ów ma tak zwany constituency, czyli obszar, który go w pierwszym rzędzie dotyczy. Te zespoły czy organizacje w sposób systemowy wymieniają się informacjami i koordynację w ramach odpowiedzi na zagrożenia czy incydenty podejmuje ten zespół, który jest najbardziej właściwy w danej sytuacji. Oczywiście, że jest tak, jeśli mamy, wynika to z ustawy antyterrorystycznej, do czynienia z zagrożeniem o charakterze terrorystycznym, to właściwą instytucją jest Agencja Bezpieczeństwa Wewnętrznego, czyli cert.gov.pl. Trudno sobie wyobrazić, żeby Minister Cyfryzacji koordynował tego typu przypadki. Żebyśmy się dobrze zrozumieli.

To, co mówiliśmy o roli koordynacyjnej w sytuacjach, w których Ministerstwo Obrony Narodowej będzie musiało podjąć określone działania... Jako że cyberprzestrzeń jest jedna i możemy mieć do czynienia z różnymi zagrożeniami o różnym charakterze, to oczywiście Ministerstwo Obrony Narodowej będzie to koordynowało.

Mówiliśmy o roli koordynacyjnej i pojedynczym punkcie kontaktowym i tak naprawdę chodzi o rolę, która wynika z dyrektywy. Chodzi o to, żeby na poziomie kraju był wyznaczony jeden podmiot, z którym można się kontaktować i który kontaktuje się z podobnymi podmiotami w innych krajach. Jedną z ważnych do spełnienia ról, jaką ma taki punkt jest w pewnym sensie synchronizacja pomiędzy sektorami i wymaganiami w poszczególnych krajach. Po to, żeby nie było tak, że wymagania dla sektora energetycznego w Polsce wynikające z ustawy o krajowym systemie, są odmienne od tego, jakie ten sam przedsiębiorca ma w innych krajach. Jest to kwestia synchronizacji pomiędzy krajami po to, żeby mieć podobne interpretacje, jak się powinno postępować. Chodzi też o przekazywanie informacji o incydentach transgranicznych. Jeśli jest incydent, który ma charakter transgraniczny, a wiemy, że teraz jest tak bardzo często, to jest ważne, żeby można było zapytać w jednym punkcie, co wiadomo na ten temat. Ten punkt powinien mieć informację. To nie znaczy, że musi on akurat koordynować samo rozwiązywanie problemów na tym poziomie operacyjnym.

Wracam do kolejnych pytań. O roli koordynatora, o odgrywaniu kluczowej roli już troszeczkę mówiłem. Chyba nic więcej nie trzeba mówić. Model, który przyjmujemy, ma szansę sprawdzić się w praktyce. Jeśli po jakimś czasie strategia zostanie ewaluowana, tak jak mówił pan dyrektor, i okaże się, że są potrzebne jakieś korekty, to będziemy mądrzejsi o doświadczenia z życia.

W gruncie rzeczy zakładany przez nas podział komptencji jest zdywersyfikowany. Można by sobie wyobrazić, że powołujemy jeden organ właściwy dla wszystkich sektorów w danym kraju. Proponujemy inny model. Mówimy, że owe sektory same najlepiej znają swoją specyfikę, więc delegowanie kompetencji w zakresie tworzenia wymogów dla tych sektorów do ministerstw czy regulatorów jest w naszym pojęciu podejściem bardziej nowoczesnym. Jest bowiem bliżej specyficznych kompetencji, które mają sektory. Spójrzmy np. na podsektor transportu lotniczego, który jest bardzo ważny, z bardzo szczególną specyfiką.

Było pytanie, jak się ma zdolność do przeciwdziałania zagrożeniom do prawa do prywatności, czyli konieczności zapewnienia obywatelom, użytkownikom cyberprzestrzeni prawa do korzystania z niej zgodnie z regułami państwa demokratycznego. Jest to oczywiście bardzo istotny temat, który pochłonął wiele debat, natomiast, jeśli spojrzymy na założenia owego dokumentu strategicznego, to prawie na samym początku jest napisane, że to wszystko, o czym mówimy i co będziemy wdrażać nie może tego porządku naruszać; nie może narażać na ograniczenia jakichkolwiek praw. Tak naprawdę bowiem chodzi o to, żeby były usługi. Na poziomie Unii Europejskiej mówi się o jednolitym rynku cyfrowym. Jest to więc kwestia ekonomiczna i gospodarcza – żeby stymulować rynek.

Rynek cyberbezpieczeństwa jest troszeczkę inny. Mówię tu w ogóle o rynku usług cyfrowych. Z punktu widzenia Ministerstwa Cyfryzacji, które jednocześnie jest liderem w budowaniu obrazu jednolitego rynku cyfrowego, jest niezwykle ważnym aspektem, żeby to zapewnić. I nie jest to hasło. Doskonale rozumiemy, że pewne kompromisy są czasem potrzebne, ale w granicach prawa i najlepiej w ramach umowy społecznej; że się na to godzimy. W ten sposób chcemy działać.

Świetne jest pytanie o to, czy przeciwdziałanie cyberprzemocy i zagrożeniom miękkim, z jakimi mamy do czynienia, jest w obszarze. Jak najbardziej jest. W prezentacji koncentrowaliśmy na technologicznym cyberbezpieczeństwie, ale jest też wiele od lat prowadzonych w kraju działań na rzecz zwiększenia safety, czyli bezpieczeństwa młodych użytkowników internetu czy przeciwdziałania zagrożeniom związanym z cyberprzemocą i wszelkimi formami wykorzystywania cyberprzestrzeni do tego, żeby stwarzać zagrożenie innym osobom. Jak najbardziej więc, jeśli spojrzymy bardziej szczegółowo na plan działań, są tam przewidziane kampanie, programy oraz oczywiście edukacja. Chodzi o stworzenie programów edukacyjnych, które będą na wielu szczeblach. Często jest bowiem tak, że mówimy o edukacji dzieci, a okazuje się, że młodzież wie o tech-

nologii więcej niż nauczyciele i rodzice. Jest więc kwestia tego, żeby umieć rozmawiać pokoleniowo. Są badania, jak młodzież korzysta z internetu. Pytanie, czy my to znamy i czytamy. Nam może się coś wydawać, że jest tak, czy inaczej, a badania często pokazują rzecz dogłębnie inną.

Od 2005 r. Polska bierze udział w programie Komisji Europejskiej, który kiedyś nazywał się Safer Internet, a teraz jest to finansowane w ramach CEF, czyli The Connecting Europe Facility. Jest to moim zdaniem jeden z najbardziej udanych projektów Komisji Europejskiej, ponieważ bardzo szybko spowodował powstanie w każdym kraju Unii Europejskiej tzw. hotline'u, czyli punktu do zgłaszania nielegalnych treści, zachowań typu cyberprzemoc. W Polsce oczywiście takie centrum także istnieje od 2005 r. Konkludując, jest to element, który widzimy jako niedoceniany aspekt. Mówimy o wojnach hybrydowych; to wszystko prawda, te zagróżenia są i istnieją. Pytanie jest o to, kto będzie chronił obywatela. Dziękuję.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Czy są jeszcze jakieś pytania bądź komentarze? Bardzo proszę, teraz pan przewodniczący Czarnecki, a później pani.

Poseł Witold Czarnecki (PiS):

Mam pytanie dotyczące finansowania. Panie ministrze, Narodowe Centrum Bezpieczeństwa działa w ramach NASK, czyli Narodowej i Akademickiej Sieci Komputerowej. Czy ma działać? A ta jest finansowana w ramach budżetu, czyli jakieś środki są przeznaczane. Nie są nazywane środkami na cyberbezpieczeństwo, ale są przeznaczane na NASK, a w jego ramach działa Narodowe Centrum Bezpieczeństwa. Jakieś finansowanie więc jest. Rozumiem, że nie jest tak, że niczego w budżecie nie ma. To się nie nazywa wprost, ale odbywa się przez finansowanie NASK, czyli Narodowej i Akademickiej Sieci Komputerowej. Tylko to chciałem uzupełnić. Dziękuję.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo panią proszę. Proszę się przedstawić.

Członek zarządu Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Bardzo dziękuję. Nazywam się Joanna Karczewska. Reprezentuję stowarzyszenie ISACA, czyli osoby, które na co dzień zajmują się bezpieczeństwem informacji, cyberbezpieczeństwem i ochroną danych osobowych. Mam pytanie związane z ochroną danych osobowych. Jednocześnie zbliża się ustawa o ochronie danych osobowych. Terminy mamy narzucone przez rozporządzenie o ochronie danych osobowych. Z drugiej strony jest dyrektywa NIS, która w art. 2 ma wymienione przetwarzanie danych osobowych. Co dla nas na co dzień ma się stać priorytetem?

Oczywiście nie ma dziś ochrony danych osobowych bez cyberbezpieczeństwa. Niemniej terminy mamy narzucone: 25 maja przyszłego roku musimy być gotowi. W takim razie, czy pojedynczy punkt kontaktowy, o którym panowie mówili, będzie też dotyczył zgłaszania naruszeń ochrony danych osobowych? Skądinąd w projekcie ustawy jest, że taki punkt powstanie przy urzędzie ochrony danych osobowych.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Bardzo proszę.

Przedstawiciel Polskiej Izby Informatyki i Telekomunikacji Daniel Ślęzak:

Dzień dobry, nazywam się Daniel Ślęzak. Reprezentuję Polską Izbę Informatyki i Telekomunikacji. Panie ministrze, podkreślana była rola uświadamiania użytkowników w zakresie bezpieczeństwa w cyberprzestrzeni od najmłodszych lat. Czy krajowe ramy przewidują wsparcie w edukowaniu osób, które miałyby nam zapewnić cyberbezpieczeństwo? Jest to powszechną bolączką, na którą wskazywała nawet minister Streżyńska. Chodzi o pozyskanie osób z odpowiednią wiedzą, doświadczeniem i o właściwych kompetencjach do wypełniania wszystkich obowiązków i zapewniania państwu oraz firmom bezpieczeństwa na adekwatnym poziomie.

Wiem, że na uczelniach są takie kierunki, ale wydaje mi się, że dziś... Jest to zauważalne też w innych krajach europejskich, ale jest to zbyt mało eksponowane. Być może

przydałby się system zachęt dla młodych ludzi, żeby wybierali tego rodzaju kierunki. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Dziękuję bardzo. Pan się zgłasza, bardzo proszę.

Wiceprezes Polskiego Towarzystwa Informatycznego Janusz Żmudziński:

Nazywam się Janusz Żmudziński, reprezentuję Polskie Towarzystwo Informatyczne. Mam pytanie do pana ministra, dotyczące wdrożenia ustawy o cyberbezpieczeństwie. Czy Ministerstwo Cyfryzacji w ramach tej ustawy ma w planach opracowanie wymagań, standardów, wytycznych dla budowania bezpiecznych systemów informatycznych? Analizując strategie, można odnieść wrażenie, że autorzy koncetrują się przede wszystkim na reagowaniu na incydenty.

Jak wiemy z praktyki jedną z przyczyn zaistnienia incydentu są błędy w budowie systemów informatycznych, zarówno w sferze technologicznej, jak i organizacyjnej. Jeżeli przeanalizujemy zapisy wymagań dla systemów informatycznych, zwłaszcza w administracji publicznej, można odnieść wrażenie, że w ramach tych systemów albo nie mamy żadnych wymagań dotyczących cyberbezpieczeństwa albo mamy je sformułowane słabo lub błędnie. Czy Ministerstwo ma jakieś plany w tym obszarze? Dziękuję.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Czy są jeszcze jakieś pytania? Jeśli nie ma, to zamykam listę. Bardzo proszę, nigdy nie odmawiam policji.

Dyrektor Biura do Walki z Cyberprzestępczością Komendy Głównej Policji Dominik Rozdziałowski:

Dziękuję, panie przewodniczący. Komisarz Dominik Rozdziałowski, jestem dyrektorm Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. Proszę państwa, chciałbym tylko zasygnalizować panu ministrowi i panu przewodniczącemu zwrócenie uwagi na dwie rzeczy.

Tak naprawdę na spotkaniach zapoznawałem się dokumetami, związanymi z ustawą wielokrotnie. Proszę państwa, cały czas mówicie o cyberincydentach, o cyberzdarzeniach i próbujecie to zdefiniować. Zgodnie z polskim prawem, każdy urząd i organ administracji państwowej, który dowie się o popełnionym przestępstwie, ma obowiązek je raportować. Dla mnie wszystkie cyberincydenty, które wymieniacie, w 80% będą przestępstwami. Z doświadczenia w pracy nad tą ustawą i nad tym, co jest w dokumentach – mam nadzieję, że będzie inaczej – wiem, że nie ma to nic wspólnego z łapaniem przestępców, którzy będą sprawcami cyberincydentów. Pamiętajcie, że jeśli po pierwszym cyberincydencie, który wydarzy się w danej sieci telekomunikacyjnej czy innej, my nie posprzątamy – proszę się nie złościć na kolokwializm, ale tak jest dosłownie – to będziecie ich państwo mieli kilka tysięcy.

Wiecie państwo doskonale, że ta przestępczość i te zdarzenia nie mają granic. Co ciekawe, wbrew powszechnym opiniom, to, że ich nie mają, to nie jest żaden problem. Wszyscy uważają, że nie ma współpracy międzynarodowej, że to jest ciężkie dla policji. Nieprawda. Współpraca jest. Dzisiaj od rana 7 chińskich policjantów pracuje cały dzień z policjantami z Polski. Mieliśmy świetne ćwiczenie w NASK, które pokazały, jak fajnie to może wyjść. Dzisiaj pracują też z nami policjanci z Islandii. Transgraniczność i to, że jesteśmy online, są przeloty sprawiają, że możemy świetnie współpracować.

Mam wrażenie, że ta ustawa kompletnie zapomniała o organach ścigania i o tym, że polskie organy ścigania pracują dwutorowo. Mamy postępowania przygotowawcze i tzw. proces, ale pamiętajmy, że są to długotrwałe terminy, wpływające czasochłonnie na wielomiesięczne prowadzenie spraw. Mamy też pracę operacyjną, którą mogą prowadzić policja i pozostałe służby, np. straż graniczna i pozostałe jednostki podległe m.in. Ministerstwu Sprawiedliwości, których przedstawicieli nigdzie nie widzę. To jest pierwsza sprawa, na którą chciałbym zwrócic uwagę pana ministra i pana przewodniczącego. Brak tych rzeczy będzie powodował, że cyberincydentów będzie tyle samo.

W pierwszych wersjach ustawy, ona się zmieni, bo jak znam pana ministra, jego charakter i siłę do pracy, to wiem, że będzie jeszcze inaczej... Chciałbym zwrócić natomiast

uwagę, że jest dużo o wymianie informacji, panie przewodniczący. Chodzi o adresy IP, logi... Ja sobie wyobrażam to tak dokładnie, że dane osobowe, o których państwo mówią, i nadzór nad jednostkami podległymi Ministerstwu Cyfryzacji będzie sprawował minister cyfryzacji. To jest dla mnie nie do końca zrozumiałe. Kiedy my uzyskujemy dane telekomunikacyjne czy dane osobowe, mamy od tego odpowiednie organy takie jak sądy, które regularnie nas sprawdzają, czy są to zasadne rzeczy. Tak samo jest z danymi osobowymi. Mamy głównego inspektora, mamy NIK, a w tych dokumentach jest mowa, że Minister Cyfryzacji sam będzie kontrolował, czy jego organy dobrze pracują. Jest to dla mnie troszkę wątpliwe, panie przewodniczący, panie ministrze. Chciałbym to tylko poddać pod rozwagę.

Przewodniczący poseł Paweł Pudłowski (N):

Świetne dwa punkty, bardzo dziękuję. Teraz tylko odpowiedzi.

Podsekretarz stanu w MC Krzysztof Silicki:

Dziękuję bardzo za kolejną porcję pytań. Odpowiadając panu przewodniczącemu, warto tutaj posłużyć się określeniem finansowanie pośrednie. Tak jak mówiliśmy oprócz dedykowanych procedur bezpieczeństwa nic się nie dzieje, bo obecnie jest tak, że w każdym projekcie informatycznym powinien występować komponent cyberbezpieczeństwa.

Mówiąc o systemie poziomu krajowego, wydaje się jednak, że przydałby się dedykowany budżet, żeby to stworzyć i skonfigurować właściwie, żeby to służyło wielu interesariuszom. Narodowe Centrum Bezpieczeństwa to jest pion w Instytucie Badawczym NASK i w zasadzie funkcjonowanie tego centrum, współpraca z przedsiębiorcami odbywa się dobrowolnie. Po prostu, jeśli dany przedsiębiorca widzi korzyść we współpracy z NC Cyber, to z niej korzysta. Współpraca taka nie ma charakteru komercyjnego. Zgadzam się w zupełności, że o budżecie trzeba mówić ostrożnie, bo różne typy finansowania powinny zaistnieć. Czym innym jest platforma narodowa, platforma cyberbezpieczeństwa, czyli projekt badawczo-rozwojowy, który ma się zakończyć konkretną implementacją, a czym innym jest pokrywanie kosztów pracy operacyjnej pierwszej, drugiej, trzeciej linii reagowania w Centrum. Takich kosztów z projektów NCBR się nie sfinansuje. Jest to dość skomplikowane.

Teraz pytanie pani doktor Karczewskiej na temat ochrony danych osobowych w relacji do dyrektywy itd. Obecnie jesteśmy w takim ciekawym momencie, że terminy zgodności z prawem Unii Europejskiej dotyczą kilku obszarów. Jest obszar wynikający z dyrektywy NIS, obszar wynikający z rozporządzenia o ochronie danych osobowycht, tj. RODO. Jest również rozporządzenie o usługach zaufania. We wszystkich wspomnianych dyrektywach czy rozporządzeniach jest podobny schemat, bo to było zamierzenie Komisji Europejskiej wyrażone po raz pierwszy w 2009 r. w pakiecie telekomunikacyjnym. Przewidziano takie mechanizmy, jak: zgłaszanie incydentów, zagrożeń, modyfikacja – różnie można o tym mówić. To jeden z mechanizmów, który jest wspólny, inaczej zdefiniowany, kogo innego dotyczy, ale sam mechanizm jest bardzo podobny. Marzyłoby się, o czym wspominaliśmy, żeby to tak zsynchronizować, aby obowiązek modyfikacyjny mógł być jak najmniej uciążliwy dla przedsiębiorców czy obywateli. Będziemy pracować nad synchronizacją. Mam nadzieję, że to się uda w którymś momencie.

Natomiast presja terminów wdrażania poszczególnych regulacji i dyrektyw nie pomaga. Z jednej strony słyszymy, że będą określone wskazówki ze strony Komisji Europejskiej, z drugiej – że musimy po prostu dotrzymać terminu. Tak jak mówiłem, 21 miesięcy na transpozycję tego typu dyrektywy to nie jest strasznie dużo.

Pytanie na temat kompetencji, szkoleń i eksponowania tego w krajowych ramach... Rozumiem, że to z Izby. Może oddałbym głos panu dyrektowi.

Dyrektor departamentu MC Piotr Januszewicz:

Jeżeli chodzi o ujęcie tego problemu w Krajowych Ramach Cyberbezpieczeństwa, to bardzo mocno koncentrowaliśmy się na tym obszarze. Wszyscy ci, którzy pracowali nad tym dokumentem, mogą to potwierdzić, a jest ich dużo na tej sali. Już w założeniach było takie hasło „złota setka”, czyli iluś ekspertów, którzy będą utrzymywani w administracji publicznej, ale to tylko obszar, który zabezpiecza administrację publiczną. Zidentyfikowaliśmy natomiast problemy, i nie tylko my, ale i na poziomie Unii Europejskiej i całego

świata, że ekspertów brakuje i będzie ich brakowało coraz więcej. W związku z tym musimy podjąć kroki w celu dostarczenia, przepraszam za kolokwializm, odpowiednich ekspertów na rynek.

Owo dostarczenie może się odbyć tylko i wyłącznie poprzez system edukacji na poziomie uczelni wyższych. Uczelnie wyższe, widząc zysk ekonomiczny w pozyskaniu studentów, otwierają kierunki. Ostatnio kierunki inżynierskie otworzyła Politechnika Warszawska. W Wyższej Szkole Policji w Szczytnie uruchomiono kierunki dotyczące cyberbezpieczeństwa. Zamierzeniem naszym jest, żeby na wszystkich uczelniach technicznych w Polsce stworzyć laboratoria cyberbezpieczeństwa. Chcemy je zasilać informacjami o zdarzeniach, które się odbyły, są znane i rozwiązane – żeby studenci w laboratoriach mieli na czym ćwiczyć.

W ramach współpracy, która odbyła się przy okazji Narodowego Centrum Bezpieczeństwa między NASK a podmiotami prywatnymi i firmami, chcemy zachęcić firmy do współpracy bezpośrednio z uczelniami; żeby uczelnie kształciły profilowane kadry inżynierskie na realizację zadań w przedsiębiorstwach. Z pierwszych rozmów, które przeprowadziliśmy z kilkoma partnerami z Narodowego Centrum Bezpieczeństwa wynika, że są tym żywotnie zainteresowani. Uważamy, że nauczanie kadr inżynierskich rzeczy praktycznych też ma swój sens, dlatego że kadry inżynierskie, które trafią bezpośrednio do owych podmiotów, będą realizowały zadania. Program ten trzeba rozszerzyć na wszystkie uczelnie techniczne, stworzyć skoordynowane działania w zakresie edukacji, a także przygotować, nie chciałbym używać sformułowania minimum programowe, bo tego się obecnie nie realizuje, ale chodzi o kompetencje, które powinien posiadać absolwent, tj. wymogi kształcenia. Myślimy o tym bardzo mocno.

Oczywiście myślimy także o tym, co się stanie, kiedy absolwent opuści uczelnię. Musi on podlegać stałemu procesowi doskonalenia zawodowego. O tym wiedzą przedstawiciele Izby, rozmawialiśmy o tym. Chcemy doprowadzić do sytuacji, w której powstanie system certyfikacji zawodowych w określonych, bardzo wąskich obszarach. Chodzi o dogłębnie kształcone kadry inżynierskie, które już pracują. Takie systemy istnieją już na świecie, w Polsce też, ale chcemy to uregulować.

Kolejną kwestią, którą w zakresie owych kadr chcemy uregulować, jest nazewnictwo, wprowadzenie zawodów. A to dlatego, że wielu zawodów na dzień dzisiejszy nie ma, nie istnieją. Gdybyśmy zapytali Główny Urząd Statystyczny, ilu jest w kraju informatyków, odpowiedziałby, że nie ma kogoś, kto nazywa się „informatyk", nie ma takiego zawodu. Uczelnie mogą oczywiście dodawać różne tytuły, ale jest to kwestia klasyfikacji zawodowych i po prostu tego nie ma. Chcemy uregulować sprawę z zawodami, zrobić ich klasyfikację. Wtedy będziemy mogli z punktu widzenia państwa dobrze zarządzać kadrami. Jeżeli będziemy mieli statystykę do kadr, będziemy wiedzieli, ile ich jest, o jakich kompetencjach. Badając zapotrzebowanie przedsiębiorców, będziemy wiedzieli, jakie kadry powinny do nich trafić. Będzie to doskonałe źródło informacji dla uczelni, jakie aktywności podjąć, żeby tego typu kadry dostarczać.

Jeśli jestem już przy temacie szkolenia, to pozwolę sobie, panie ministrze, na sekundę wrócić do edukacji. Ministerstwo Edukacji Narodowej przy dużym zaangażowaniu Ministerstwa Cyfryzacji wprowadziło do programów nauczania w szkołach podstawowych elementy cyberbezpieczeństwa. Wywieraliśmy na to duży nacisk, dlatego że tak jak od najmłodszych lat uczymy młodzież przepisów ruchu drogowego, tak samo musimy uczyć bezpiecznego korzystania z nowoczesnych technologii. Ma się to odbywać na jak najwcześniejszym etapie edukacji. Wracam do tego pytania, żeby uzupełnić. To tyle, jeśli chodzi o temat kadr i młodzieży.

Podsekretarz stanu w MC Krzysztof Silicki:

Kolejne pytanie dotyczyło tego, czy koncetrujemy się wyłącznie na reagowaniu czy działamy w kierunku tworzenia wymogów i standardów. To może też pan odpowie, panie dyrektorze.

Dyrektor departamentu MC Piotr Januszewicz:

Miałem swego czasu taki rysunek, który pokazywałem chyba w Centrum Cyberprzestrzeń i mówiłem, co rozumiemy przez bezpieczną cyberprzestrzeń. Bezpieczna to zna-

czy taka, która jest dobrze zbudowana – security by design. Ja wolę nazywać to, tak jak się mówiło kiedyś, architekturą zorientowaną na bezpieczeństwo i usługi – service oriented architecture. Proponuję dodać kolejne „s" na bezpieczeństwo. Zgadzamy się w zupełności i rozumiemy to, dlatego że system, który zostanie zaprojektowany bez myślenia o bezpieczeństwie, tak naprawdę jest skompromitowany w pierwszych próbach eksploatacyjnych. Później dokładanie bezpieczeństwa kończy się albo wycofaniem go z eksploatacji, ponieważ nie da się zaimplementować bezpieczeństwa, albo dużymi nakładami, które czasami przekraczają nakłady poniesione na jego zaprojektowanie.

Uważamy więc, że do ochrony powinny być oddane systemy, które są prawidłowo zbudowane. Zawsze stosuję odniesienie do budownictwa. Jak mamy dobrze zbudowany budynek, to jego utrzymanie niewiele kosztuje, bo się nie zawali. Tak samo jest z systemami teleinformatycznymi. Jeżeli rozwiązania systemu będą prawidłowo zrealizowane, to ochrona systemu będzie zdecydowanie tańsza, a przede wszystkim realizowalna.

Druga rzecz, o której mówimy w strategii bardzo mocno i czego nie ma w innych strategiach, to bezpieczny łańcuch dostaw. Urządzenia i oprogramowanie, które wykorzystujemy do budowy nawet najlepiej zaprojektowanych systemów, muszą spełniać wymogi. I tu znów odwołanie do budownictwa: wszystkie materiały budowlane – cegły, pustaki, elementy stropu, beton – muszą mieć odpowiednie certyfikaty i spełniać normy jakościowe. To samo musimy stosować w przypadku systemów teleinformatycznych. Dla pewnych infrastruktur, które są istotne z punktu widzenia funkcjonowania państwa, powinniśmy wykorzystywać rozwiązania, które są sprawdzone, przetestowane i mają odpowiednie czy certyfikaty bezpieczeństwa, czy znamy ich pochodzenie i wiemy dokładnie, jak były zrobione. Uważamy więc, że muszą zaistnieć te dwa elementy: architektura zorientowana na bezpieczeństwo i usługi oraz bezpieczny łańcuch dostaw, czyli komponenty, z których budujemy. Dopiero taki system możemy przekazać do eksploatacji, bo będzie go można skutecznie bronić.

Przewodniczący poseł Paweł Pudłowski (N):

Jeszcze są zgłaszane uwagi.

Podsekretarz stanu w MC Krzysztof Silicki:

W odpowiedzi na pytania pana komisarza Rozdziałowskiego, nie zapominamy o tym, że cyberincydenty, nazywane tak przez zespoły typu CERT, są przestępstwem. Natomiast w tym systemie, który był tutaj opisywany, można znaleźć interfejsy pomiędzy reagowaniem na zgłoszone incydenty a potem przekazywaniem ich do organów, które zajmują się ściganiem przestępców. CERT-y nie ścigają przestępców, natomiast mogą służyć wszelkimi analizami technicznymi, które są potrzebne do tego, aby przeanalizować naturę danego ataku itd. itd. Jeśli jest takie odczucie, że nie jest to wystarczające podkreślone, to przyjmujemy tę uwagę. Na pewno nie było naszą intencją, żeby o tym zapominać.

Wspomniał pan o ćwiczeniach w NC Cyber, gdzie specjaliści z CERT-u, policji i prokuratury siedzieli razem i na podstawie konkretnych przypadków podejmowali wspólne działania po to, żeby szybko przejść do fazy, w której policja wraz z prokuraturą może rozpocząć ściganie przestępcy. Nie chcemy o tym zapomnieć i nie zapomnimy.

Jeśli chodzi o kontrolę nad jednostkami, poprosiłbym o odpowiedź paną dyrektor Katarzynę Prusak-Górniak.

Dyrektor Departamentu Prawnego w MC Katarzyna Prusak-Górniak:

Dziękuję bardzo. Katarzyna Prusak-Górniak, jestem dyrektorem Departamentu Prawnego. Jeżeli mogę, panie ministrze, uzupełnić pana wypowiedź, to powiem, że na bazie doświadczeń z ćwiczeń, które odbyły się w NASK-u, podjęliśmy współpracę z grupą ekspertów w celu opracowania możliwych wariantów obsługi incydentów bezpieczeństwa teleinformatycznego, ze szczególnym uwzględnieniem roli organów ścigania i władzy sądowniczej. Dotyczyły one zagadnienia współpracy między organami samorządowymi a operatorami usług kluczowych i dostawcami usług cyfrowych. Mam nadzieję, że pod koniec tego roku będziemy mieli gotowe propozycje, w jaki sposób zaadresować tę procedurę obsługi incydentów. Zobaczymy, w jaki sposób zdążymy. Naszym priorytem jest na razie wdrożenie dyrektywy NIS.

Dyrektor biura KGP Dominik Rozdziałowski:

Przepraszam bardzo. Wiedzą państwo, że ci ludzie w momencie wejścia ustawy nie powiadamiając organów ścigania o przestępstwach, w większości sami będą je popełniali? Będziemy gotowi?

Dyrektor departamentu MC Katarzyna Prusak-Górniak:

Jednak obowiązek zawiadamiania o przestępstwach wynika już z poprzednio obowiązujących przepisów. Nie ma potrzeby wprowadzania tą ustawą kolejnych obowiązków, ponieważ ten obowiązek już istnieje. Jest kwestia uproszczenia i uelastycznienia procedur. Wraz z grupą ekspertów pracujemy nad propozycjami takiego uelastycznienia, ale żeby wypracować docelowe rozwiązanie będzie to wymagało współpracy z państwem. My chcemy zaproponować jakieś rozwiązanie, żeby mieć nad czym pracować.

Natomiast co do pytania dotyczącego nadzoru, to będą tu miały zastosowanie zasady ogólne zakresu ochrony danych osobowych i właściwość organu ochrony danych osobowych. Minister nie będzie w tym zakresie...

Dyrektor biura KGP Dominik Rozdziałowski:

A jeżeli chodzi o dane telekomunikacyjne? Przekazywanie danych objętych pozostałymi tajemnicami: telekomunikacyjną, bankową, sektorową, zawodową?

Dyrektor departamentu MC Katarzyna Prusak-Górniak:

Tutaj będą regulacje sektorowe miały...

Dyrektor biura KGP Dominik Rozdziałowski:

Czyli w przypadku tajemnicy telekomunikacyjnej wymienianej pomiędzy operatorami, CSIRT-ami a pozostałymi jednostkami, to jak mogłoby to być kontrolowane? Przez kogo? Proszę mi wybaczyć, ja akurat w policji stoję na stanowisku, że kontrola sądów nie jest niczym uciążliwym. Wręcz przeciwnie: powoduje szereg ułatwień i wpływa na transparentnosc naszej pracy. Tutaj widzę jednak spore zagrożenie.

Jeżeli chodzi o moje dane, jako obywatela Rzeczypospolitej Polskiej, nie chciałbym, żeby bez nadzoru odpowiednich organów – sądowych czy innych wyznaczonych przez państwo polskie – były one przekazywane między operatorami, firmami zewnętrznymi, które będą w CSIRT-ach... Proszę wybaczyć, to jest zagrożenie, które widać przy pracach nad ustawą. To tylko pod państwa rozwagę.

Dyrektor departamentu MC Katarzyna Prusak-Górniak:

Dostrzegając istotność zagadnienia, o którym pan wspomina, w ramach prac w grupie roboczej, a tak jak podkreślał pan minister, współpracujemy bardzo blisko, myślę że będziemy się nad tym pochylać. Będą uzgodnienia międzyresortowe ustawy, będzie możliwość zgłoszenia wszelkich uwag, szerokiej dyskusji, będziemy to konsultować. Myślę, że wszystkie te zagadnienia i ryzyka postaramy się zaadresować.

Przewodniczący poseł Paweł Pudłowski (N):

Jeszcze się zgłasza poseł Marchewka. Bardzo proszę.

Poseł Arkadiusz Marchewka (PO):

Panie przewodniczący, panie ministrze. Rzeczywiście w prowadzonej przez ostatnią godzinę dyskusji pojawiają się pewne nieścisłości czy też kwestie, które należałoby dodatkowo doprecyzować. Osobiście uważam, że objęcie przez pana stanowiska odpowiedzialnego za cyberbezpieczeństwo było ruchem w dobrą stronę. Pokazuje to, że kwestia cyberbezpieczeństwa, szczególnie w Ministerstwie Cyfryzacji, jest istotna. Jednak, jak sam pan minister przyznał, przydałoby się jednak znaleźć dodatkowe środki na wdrażanie tych kwestii. Byłoby wtedy łatwiej.

Myślę, że temat cyberbezpieczeństwa nie jest w żaden sposób tematem politycznym. Jest czymś, co powinniśmy wspierać bez względu na to, jakie mamy poglądy i w jakich jesteśmy klubach. Dlatego myślę, że w procesie tworzenia budżetu na 2018 r. i na końcówce przygotowywania planu działań na rzecz wdrożenia krajowych ram cyberbezpieczeństwa udałoby się, przynajmniej z punktu widzenia Komisji, wesprzeć działania ministerstwa, aby takie środki finansowe znaleźć. Myślę, że nawet pan przewodniczący

Czarnecki zgodzi się ze mną, że warto byłoby poruszyć tę kwestię na którymś z kolejnych spotkań Komisji. Jest to bowiem kwestia bardzo istotna.

Trzeba odpowiedzieć na pytanie dotyczące, nie wiem czy zagarniania, czy przeznaczania większości środków finansowych albo łatwości zdobywania środków przez MON, a trudności przez Ministerstwo Cyfryzacji. Uważam, że naszą rolą jako Komisji byłoby wsparcie dążeń, aby te działania przeprowadzić. Kiedy będziemy opiniować plan budżetu na 2018 r. i równocześnie będziemy znali plan działań w zakresie realizacji Krajowych Ram Cyberbezpieczeństwa, to moglibyśmy jako Komisja podjąć działanie rekomendujące, a nawet wspierające. Warto, żebyśmy któreś z kolejnych posiedzeń Komisji temu przeznaczyli.

Słowo do pana przewodniczącego Czarneckiego: liczę, że nie będziemy się kierować w żaden sposób kwestiami politycznymi, bo to jest coś, co powinniśmy wspierać bez względu na to, gdzie jesteśmy. To jest taki mój apel, abyśmy zamknęli ten rozdział, ale wkrótce spróbowali otworzyć kolejny, kiedy więcej szczegółów będzie już znanych.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Czy są jeszcze jakieś uwagi lub pytania? Jeśli nie, zamykam dyskusję.

Stwierdzam, że porządek dzienny został wyczerpany. Zamykam posiedzenie Komisji. Protokół posiedzenia wraz załączonym zapisem jego przebiegu jest do wglądu w sekretariacie Komisji w Kancelarii Sejmu. Dziękuję państwu bardzo.